|  |
| --- |
| *Наименование органа исполнительной власти* *(или органа местного самоуправления)* |
| СОГЛАСОВАНОМинистр области – председатель комитетапо информатизации области \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Л.Ю. Кузнецова\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2015 года | УТВЕРЖДАЮ*Наименование органа власти* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Иванов \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2015 года |
| **Система защиты информации** **информационной системы персональных данных** *«Наименование ИСПДн» наименование органа власти* |
| **ТЕХНИЧЕСКОЕ ЗАДАНИЕ** СОГЛАСОВАНО РАЗРАБОТАЛ Начальник отдела ………………информационных систем ………………управления информационных ……………….технологий комитета ……………….по информатизации области ……………….\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.В. Носов \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Иванов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2015 года \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2015 года |

1. **Общие сведения**

Настоящее Техническое задание разработано в соответствии с Приказом ФСТЭК №21 от 18.02.2013, Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 а так же с учётом ГОСТ 34.602 – 89 и является, согласно ГОСТ 34.602-89, основным документом, определяющим требования и порядок создания, развития, модернизации, сопровождения Системы защиты информации информационной системы персональных данных *«наименование системы»*. Совместно со специалистами сторонней организации *«наименование организации», проводятся все работы от разработки до ввода данной системы в действие (приема-сдачи в промышленную эксплуатацию).\*[[1]](#footnote-1)*

Результатом создания Системы защиты информации информационной системы персональных данных *«наименование системы»* должна стать полностью работоспособная автоматизированная Система защиты персональных данных информационной системы персональных данных, соответствующая требованиям настоящего технического задания.

Согласно ГОСТ 34.602-89 изменения к техническому заданию (ТЗ) на создание системы защиты оформляют дополнением или подписанным заказчиком и разработчиком протоколом. Дополнение или указанный протокол являются неотъемлемой частью технического задания на Систему защиты информации информационной системы персональных данных *«наименование системы».*

**1.1 Полное наименование системы**

Полное наименование системы – «Системы защиты информации информационной системы персональных данных *«полное наименование ИСПДн, указывается без сокращений».*

Сокращенное наименование системы – СЗИ ИСПДн *«сокращенное наименование ИСПДн»*

**1.2 Наименование реквизитов разработчика и заказчика СЗИ ИСПДн.**

*В этом пункте указываются реквизиты сторон, заказчика и исполнителя*

**1.3 Перечень документов, на основании которых создаётся СЗИ ИСПДн.**

Для формирования требований были использованы документы разработанные на предыдущих этапах создания СЗИ ИСПДн, которые приведены в таблице 1.

Таблица 1. Документы, разработанные на предыдущих этапах создания СЗИ ИСПДн *«наименование системы»*

|  |  |
| --- | --- |
| № п/п | Наименование документа |
| 1  | Частная модель угроз безопасности информации для автоматизированного рабочего места информационной системы персональных данных *«наименование системы»* *наименование органа власти, «органа местного самоуправления»* |
| 2  | Акт классификации СЗИ ИСПДн *«наименование системы»*  |
| 3 | Акт определения уровня защищенности персональных данных СЗИ ИСПДн *«наименование системы»* |

Основные руководящие (РД) и нормативно – технические документы (НТД) приведены в таблице 2.

Таблица 2. Перечень основных руководящих и нормативно технических документов.

|  |  |
| --- | --- |
| № п/п  | Наименование документа  |
| 1  | ГОСТ 34.003-90 Автоматизированные системы. Термины и определения  |
| 2  | ГОСТ 34.602-89 Техническое задание на создание автоматизированной системы  |
| 3  | ГОСТ 34.603-92 Виды испытаний автоматизированных систем  |
| 4  | ГОСТ 34.601-90 Автоматизированные системы. Стадии создания  |
| 5  | ГОСТ 34.201-89 Виды, комплектность и обозначения документов при создании автоматизированных систем  |
| 6  | РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов  |
| 7  | ГОСТ 19.505-79 Руководство оператора. Требования к содержанию и оформлению  |
| 8  | ГОСТ 19.503-79 Руководство системного программиста. Требования к содержанию и оформлению  |
| 9 | Требования ФСБ «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» |
| 10 | Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21) |
| 11 | Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119) |

Плановые сроки начала и окончания работ по созданию системы защиты информации *«указать плановые сроки»*

**2. Назначение и цели создания системы**

**2.1 Назначение системы защиты.**

СЗИ ИСПДн *«наименование системы»* предназначена для*…… описать для чего предназначена система.*

**2.1 Цели создания системы защиты**

Целями создания системы защиты ИСПД является:

*Указать цели создания системы защиты.*

СЗИ ИСПДн *«наименование системы»* предполагается использовать в информационной системе персональных данных *«наименование системы» наименование органа власти или местного самоуправления.*

Критерием оценки достижения целей создания системы является снижение величины наносимого ущерба вследствие реализации угроз безопасности, путём применения технических, организационных мер, надлежащее выполнение требований безопасности, предусмотренных нормативно-методическими документами для ИСПД с заданными параметрами.

**2.2 Краткая характеристика информационной системы, структура**. *Описать характеристику системы, что из себя представляет. Где находятся технические средства ИСПДН за пределами РФ и в пределах РФ.*

**2.3 Размещение СЗИ ИСПДн *«наименование системы».***

СЗИ ИСПДнрасположен по адресу*: указать фактический адрес установки системы, рабочего места.*

**2.4 Охрана и пропускной режим.**

 *Как осуществляется пропускной режим на объект где установлена ИСПДн. «есть ли охрана, установлена ли сигнализация, решетки на окнах, железная дверь, ведется ли опечатывание и.т.д.»*

**2.5 Контролируемая зона.**

 Контролируемая зона представлена в виде периметра стен помещения *«номер помещения, если нет номера, то указываем его название» в котором находится* СЗИ ИСПДн *«наименование системы».*

**2.6 Схема информационного взаимодействия объектов ИСПДн *«наименование системы».***



*Пример.* Рисунок 1. Схема информационного взаимодействия объектов распределенной ИСПД *«наименование системы»*

*Пример.* Рисунок 2. Схема информационного взаимодействия объектов локальной ИСПД *«наименование системы»*

**2.7. Уровень защищенности персональных данных в ИСПДн *«наименование системы»***

Комиссией по определению уровня защищенности персональных данных в ИСПД *«наименование системы»* установлен уровень защищенности персональных данных \_\_\_\_ *указать номер уровня защищенности из акта определения УЗ.*

**2.8. Частная модель угроз безопасности персональных данных в ИСПДн *«наименование системы»***

*Вставить перечень актуальных угроз безопасности персональных данных в ИСПДн «наименование системы»*

**3 Требования к системе защиты информации информационной системы персональных данных *«наименование системы»***

**3.2 Требования к функциям (задачам), выполняемым системой.**

*Для ИСПДн относящихся к классу «иные» необходимо применять приказ ФСТЭК России от 18 февраля 2013 года №21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».*

*Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:*

*- определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в* [*таблице 3*](#Par126)*;*

*- адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);*

*Для обеспечения 3 уровня защищенности персональных данных применяются:*

*средства вычислительной техники не ниже 5 класса;*

*системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;*

*межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;*

*Для обеспечения 4 уровня защищенности персональных данных применяются:*

*средства вычислительной техники не ниже 6 класса;*

*системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;*

*межсетевые экраны 5 класса.*

*Таблица 3. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней*

*защищенности персональных данных. (Приложение к Приказу ФСТЭК*

*от 18 февраля 2013 г. № 21 «об утверждении состава и содержания*

*организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».*

|  |  |  |
| --- | --- | --- |
| *Условное обозначение и номер меры*  | *Содержание мер по обеспечению безопасности персональных данных*  | *Уровни защищенности персональных данных (УЗ)* |
|  *4*  |  *3*  |  *2*  |  *1*  |

Таблица 3.1 Перечень мер защиты информации для СЗ ИСПД

| Условное обозначение и номер меры | Меры защиты информации в информационных системах | Базовый набор требований к уровню защищённости (номер УЗ) | Адаптированный базовый набор мер |
| --- | --- | --- | --- |

**4. Требования к средствам защиты.**

Средства защиты информации должны удовлетворять следующим требованиям:

- средства антивирусной защиты *– «…………»;*

- средства защиты от несанкционированного доступа – *«……………»*;

- средства безопасного межсетевого взаимодействия, средства криптографической защиты каналов передачи данных – *«……………………..»*.

Средства защиты информации, применяемые для защиты персональных данных, должны проходить процедуру оценки соответствия. Средства защиты информации должны иметь действующие сертификаты соответствия ФСТЭК России и (или) ФСБ России.

**4.1 Требования по электрической и пожарной безопасности**

Технические средства, применяемые для реализации приведённых выше требований должны соответствовать нормам по электрической и пожарной безопасности, принятым на предприятии заказчика.

Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ГОСТ 12.1.030-81 и ПУЭ.

Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование.

**4.2 Требования по эксплуатации и техническому обслуживанию**

Для нормальной эксплуатации разрабатываемой системы должно быть обеспечено бесперебойное питание ПЭВМ. При эксплуатации система должна быть обеспечена соответствующая стандартам хранения носителей и эксплуатации ПЭВМ температура и влажность воздуха. Размещение помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств. Размещение оборудования, технических средств должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности. Все пользователи системы должны соблюдать правила эксплуатации электронной вычислительной техники. Периодическое техническое обслуживание используемых технических средств должно проводиться в соответствии с требованиями технической документации изготовителей, но не реже одного раза в год.

Квалификация персонала и его подготовка должны соответствовать технической документации.

**4.3 Требования к патентной чистоте**

По всем техническим и программным средствам, применяемым в системе, должны соблюдаться условия лицензионных соглашений и обеспечиваться патентная чистота на территории Российской Федерации.

Патентная чистота – это юридическое свойство объекта, заключающиеся в том, что он может быть свободно использован в Российской Федерации без опасности нарушения действующих на ее территории патентов исключительного права, принадлежащего третьим лицам (права промышленной собственности).

**4.4 Требования к эргономике и технической эстетике**

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав системы должно осуществляться посредством визуального графического интерфейса (GUI). Интерфейс системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной системы. Ввод-вывод данных системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям системы. Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов. Клавиатурный режим ввода должен используется главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм. Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на русском языке.

 **4.5 Требования к составу и содержанию работ по созданию системы защиты информации персональных данных**.

Этапы работы по созданию АСЗИ отражены в таблице 4.

Таблица 4.

| Этап | Содержание работ\* | Результаты работ |
| --- | --- | --- |
| 1 | Разработка документов технического проекта.На основании технического задания должен быть разработан технический проект, в котором будут подробно изложены этапы создания СЗИ ИСПДн, состав закупаемых средств защиты, очерёдность их установки и проверки их функционирования, состав и компетенции обслуживающего СЗИ персонала. | Документы технического проекта СЗИ ИСПДн |
| 2 | Согласование технического проекта.Разработанный технический проект отправляется на ознакомление и согласование заказчику. В ходе этого этапа могут быть внесены дополнения и изменения в проект, если это потребуется. Итогом согласования проекта является подписание его сторонами. |  |
| 3 | Закупка средств защиты информации, указанных в техническом проекте.На этом этапе производится закупка средств защиты информации, предусмотренных техническим проектом; Средства защиты должны быть закуплены в полном объёме. | Доставка на объект заказчика закупленных средств защиты информации. |
| 4 | Установка и настройка параметров закупленных средств защиты информации.Закупленные средства защиты должны быть установлены на объекте заказчика и соответствующим образом настроены для выполнения своих функций. Настройка должна производиться специалистами, имеющими соответствующую квалификацию. | Распаковка, монтаж, подключение и настройка параметров средств защиты на объекте заказчика. |
| 5 | Проведение испытаний созданной системы защиты информации | Акт ввода в опытную эксплуатацию. |
| 6 | Составление документации на автоматизированную систему защиты информации, необходимой нормативно-распорядительной документации на объекте информатизации | Технический паспорт на созданную автоматизированную систему защиты информации. Инструкция администратора систем, инструкция пользователя системы. |
| 7 | Аттестация СЗИ ИСПДн *«наименование системы»* | Программа и методика аттестационных испытанийПротокол аттестационных испытанийЗаключение по результатам аттестационных испытанийАттестат соответствия |
| 7 | Ввод системы в эксплуатацию | Акт ввода системы в промышленную эксплуатацию. |

**4.6 Требования к разработчику системы защиты**

Привлекаемый на договорной основе разработчик (юридическое лицо или индивидуальный предприниматель) должен иметь лицензию(ии) на деятельность по технической защите конфиденциальной информации и деятельность на техническое обслуживание шифровальных (криптографических) средств в соответствии с законодательством РФ.

**5. Порядок контроля и приёмки системы**

**5.1 Порядок проведения приёмки**

Испытания СЗИ ИСПДн проводятся на объекте заказчика;

Испытания могут проводиться с целью проверки как отдельной подсистемы или функционального модуля, так и на СЗИ ИСПДн в целом.

На основании решения о приемке осуществляется подписание комиссией акта приемки;

Опытная эксплуатация системы защиты ИСПД выполняется на развернутом и настроенном рабочем месте, на котором потом будет осуществляться дальнейшая промышленная эксплуатация.

**6. Перечень средств защиты информации СЗИ ИСПДн *«наименование системы».***

|  |  |  |
| --- | --- | --- |
| Наименование средств защиты информации | Количество  | Срок действия сертификата ФСБ России (ФСТЭК России) |
|  |  |  |
|  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Изм. | Номера листов (страниц) | Всего листов (страниц) в документе | № докум. | Вход. № сопровод. докум и дата | Доп. | Дата. |
| Изменённых  | Заменённых | Новых | Аннулированных |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Лист регистрации изменений

1. *ПРИМЕЧАНИЕ: Курсивом выделены комментарии, которые необходимо удалить и заменить конкретной информацией об эксплуатируемой информационной системе персональных данных (шрифт в тексте должен быть только* Times New Roman, 14, прямой)*.* [↑](#footnote-ref-1)